EP03/09063

Ministero delle Attività Produttive

Direzione Generale per lo Sviluppo Produttivo e la Competitività

Ufficio Italiano Brevetti e Marchi

Ufficio G2

REC'D 30 OCT 2003
WIPO PCT

Autenticazione di copia di documenti relativi alla domanda di brevetto per: Invenzione Industriale

N. MI2002 A 002339

10,33 Euro

Si dichiara che l'unita copia è conforme ai documenti originali depositati con la domanda di brevetto sopraspecificata, i cui dati risultano dall'accluso processo verbale di deposito.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Roma, li 30 LUG. 2003

IL DIRIGENTE

Sig.ra E. MARINELLI

BEST AVAILABLE COPY

AL MINISTERO DELLE ATTIVITÀ PRODUTTIVE
UFFICIO ITALIANO BREVETTI E MARCHI - ROMA
DOMANDA DI BREVETTO PER INVENZIONE INDUSTRIALE, DEPOSITO RISERVE, ANTICIPATA ACCESSIBILITÀ AL PUBBLICO

MODULO A

A. RICHIEDENTE (I)

1) Denominazione: STIGLIANI DOMENICO — PF
Residenza: Rimini — codice STGDNC70C[illegible]2570

2) Denominazione: STIGLIANI FAUSTINO NICOLA — PF
Residenza: Scandiano (Reggio Emilia) — codice STGFTN54E17G942C

B. RAPPRESENTANTE DEL RICHIEDENTE PRESSO L'U.I.B.M.

cognome nome: FARAGGIANA Vittorio ed altri — cod. fiscale
denominazione studio di appartenenza: Ingg. Guzzi e Ravizza s.r.l.
via: V. Monti — n. 8 — città: MILANO — cap: 20123 — (prov): MI

C. DOMICILIO ELETTIVO destinatario
via — n. — città — cap — (prov)

D. TITOLO — classe proposta (sez/cl/scl) — gruppo/sottogruppo

"METODO E DISPOSITIVI PER ESEGUIRE CONTROLLI DI SICUREZZA IN SCAMBI ELETTRONICI DI MESSAGGI"

ANTICIPATA ACCESSIBILITÀ AL PUBBLICO: SI ☐ NO ☒ — SE ISTANZA: DATA — N° PROTOCOLLO

E. INVENTORI DESIGNATI

cognome nome		cognome nome	
1) STIGLIANI DOMENICO		3) RUCCO PAOLO	
2) STIGLIANI FAUSTINO NICOLA		4)	

F. PRIORITÀ

	nazione o organizzazione	tipo di priorità	numero di domanda	data di deposito	allegato S/R
1)					
2)					

SCIOGLIMENTO RISERVE — Data — N° Protocollo

G. CENTRO ABILITATO DI RACCOLTA COLTURE DI MICRORGANISMI, denominazione

H. ANNOTAZIONI SPECIALI

DOCUMENTAZIONE ALLEGATA

	N. es.			
Doc. 1)	2	PROV	n. pag. 16	riassunto con disegno principale, descrizione e rivendicazioni (obbligatorio 1 esemplare)
Doc. 2)	2	PROV	n. tav. 01	disegno (obbligatorio se citato in descrizione, 1 esemplare)
Doc. 3)	0	~~PRIS~~ XX		lettera d'incarico, procura o riferimento procura generale
Doc. 4)	☐	RIS		designazione inventore
Doc. 5)	☐	RIS		documenti di priorità con traduzione in italiano
Doc. 6)	☐	RIS		autorizzazione o atto di cessione
Doc. 7)	☐			nominativo completo del richiedente

SCIOGLIMENTO RISERVE — Data — N° Protocollo
confronta singole priorità

8) attestati di versamento, totale Euro: CENTOTTANTOTTO/51 (188,51) — obbligatorio

COMPILATO IL 05/11/2002 — FIRMA DEL(I) RICHIEDENTE(I): p.i.
CONTINUA SI/NO si — Ingg. Guzzi e Ravizza
DEL PRESENTE ATTO SI RICHIEDE COPIA AUTENTICA SI/NO si — per sé e per gli altri

---

CAMERA DI COMMERCIO IND. ART. E AGR. DI MILANO — MILANO — codice 15

VERBALE DI DEPOSITO — NUMERO DI DOMANDA MI2002A 002339 — Reg. A.

L'anno DUEMILADUE — il giorno CINQUE — del mese di NOVEMBRE

Il(I) richiedente(i) sopraindicato(i) ha(hanno) presentato a me sottoscritto la presente domanda, corredata di n. 01 fogli aggiuntivi per la concessione del brevetto sopraripportato.

I. ANNOTAZIONI VARIE DELL'UFFICIALE ROGANTE: IL RAPPRESENTANTE PUR INFORMATO DEL CONTENUTO DELLA CIRCOLARE N.423 DEL 01/06/2001 EFFETTUA IL DEPOSITO CON RISERVA DI LETTERA DI INCARICO.

IL DEPOSITANTE

L'UFFICIALE ROGANTE

AGGIUNTA MODULO A

FOGLIO AGGIUNTIVO n. 01 di to[illegible] DOMANDA N. MI1 MI2002A[illegible]2339 REG. A

A. RICHIEDENTE (I) N.G.

03 Denominazione RUCCO PAOLO PF

Residenza Scandiano (Reggio Emilia) codice RCCPLA64D21E506Q

Denominazione

Residenza codice

Denominazione

Residenza codice

Denominazione

Residenza codice

Denominazione

Residenza codice

Denominazione

Residenza codice

E. INVENTORI DESIGNATI

cognome nome	cognome nome

F. PRIORITÀ

nazione o organizzazione	tipo di priorità	numero di domanda	data di deposito	allegato S/R
			/ /	
			/ /	
			/ /	
			/ /	
			/ /	
			/ /	

SCIOGLIMENTO RISERVE

Data	N° Protocollo
/ /	
/ /	
/ /	
/ /	
/ /	
/ /	

FIRMA DEL (I) RICHIEDENTE (I) p.i.

Ingg. Guzzi e Ravizza

per sé e per gli altri

SPAZIO RISERVATO ALL'UFFICIO CENTRALE BREVETTI

PROSPETTO A

RIASSUNTO INVENZIONE CON DISE[redacted]RINCIPALE, DESCRIZIONE E RIVENDICAZIONE

NUMERO DOMANDA MI2002A 002339 REG. A

DATA DI DEPOSITO 05 11 2002

NUMERO BREVETTO

DATA DI RILASCIO

D. TITOLO

"METODO E DISPOSITIVI PER ESEGUIRE CONTROLLI DI SICUREZZA IN SCAMBI ELETTRONICI DI MESSAGGI"

L. RIASSUNTO

Un metodo per una verifica di sicurezza di un messaggio (Msg) trasmesso e ricevuto in forma elettronica, comprende dal lato trasmittente le fasi di associare al messaggio un identificatore univoco di messaggio (ID_{Msg}) e un identificatore (ID_{CR}) di controllo della identità del titolare del messaggio, il quale è ottenuto applicando all'identificatore univoco di messaggio (ID_{Msg}) una codifica (12) associata al titolare del messaggio da trasmettere. Dal lato ricevente il metodo comprende le fasi di verificare e segnalare il fatto di avere o non avere già ricevuto precedentemente un messaggio con lo stesso identificatore univoco di messaggio (ID_{Msg}) associato e di accertare la corrispondenza fra identificatore univoco di messaggio (ID_{Msg}) associato al messaggio ricevuto e risultato (ID_{DCR}) di una decodifica dell'identificativo di controllo (ID_{CR}). Un sistema e un dispositivo di verifica secondo il metodo sono anche descritti.

M. DISEGNO

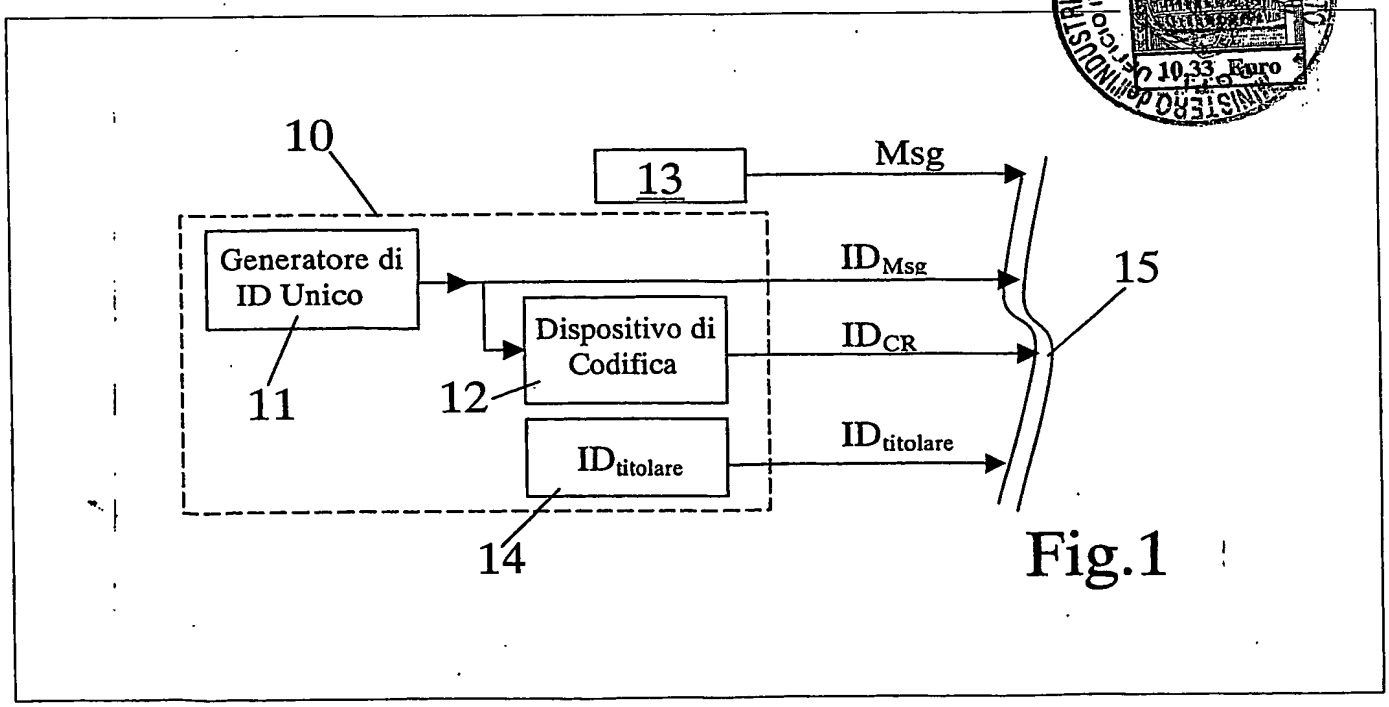


Fig.1

"Metodo e dispositivi per eseguire controlli di sicurezza in scambi elettronici di messaggi"

MI 2002A 002339

titolari: 1) STIGLIANI DOMENICO 2) STIGLIANI FAUSTINO NICOLA 3) RUCCO PAOLO

residenti in: 1) Rimini 2) e 3) Scandiano (Reggio Emilia)

******

La presente invenzione si riferisce ad un metodo e a dispositivi per eseguire controlli di sicurezza in scambi elettronici di messaggi, in particolare per transazioni monetarie, quali quelle eseguite con carte di credito o di debito e simili.

Sono noti i problemi di sicurezza presenti nello scambio in forma elettronica di messaggi, specialmente su reti intrinsecamente insicure, come sono ad esempio le reti formanti Internet.

Fra i vari problemi si possono elencare la possibilità che qualcuno generi messaggi (in particolare, richieste di transazioni monetarie) falsificando il titolare del messaggio, e la possibilità che vengano duplicati messaggi reali per ottenere che una richiesta contenuta nel messaggio venga nuovamente soddisfatta.

Nella tecnica nota si è tentato di porre rimedio ad alcuni aspetti di tali problemi, ad esempio con l'introduzione di sistemi quali la cosiddetta "firma elettronica" che permette però di avere la ragionevole certezza della identità del titolare del messaggio, ma non della unicità del messaggio stesso.

I sistemi noti sono comunque in genere complessi, di difficile applicabilità, e/o generano un sovraccarico nella elaborazione e/o trasmissione dei messaggi che non sempre sono accettabili, specialmente nel caso di applicazioni che producono e devono gestire un elevatissimo numero di messaggi in tempi relativamente ridotti, quale ad esempio è il caso delle transazioni monetarie tramite carta di credito o di debito, specialmente se impiegate per il pagamento di beni o servizi su internet o

presso negozi con terminali POS o similari.

Scopo generale della presente invenzione è ovviare agli inconvenienti sopra menzionati fornendo un metodo e dispositivi per la verifica di sicurezza nello scambio di messaggi per via elettronica, che siano rapidi, facilmente applicabili e di elevata affidabilità intrinseca.

In vista di tale scopo si è pensato di realizzare, secondo l'invenzione, un metodo per una verifica di sicurezza di un messaggio trasmesso e ricevuto in forma elettronica, il quale dal lato trasmittente comprende le fasi di associare al messaggio, per la sua successiva verifica di sicurezza, un identificatore univoco di messaggio e un identificatore di controllo della identità del titolare del messaggio, l'identificatore di controllo essendo ottenuto applicando all'identificatore univoco di messaggio una codifica associata al titolare del messaggio da trasmettere; dal lato ricevente, per la verifica di sicurezza di un messaggio ricevuto, comprende le fasi di verificare e segnalare il fatto di avere o non avere già ricevuto precedentemente un messaggio con lo stesso identificatore univoco di messaggio associato; applicare una decodifica, associata ad un supposto titolare del messaggio ricevuto, all'identificatore di controllo del titolare associato al messaggio ricevuto; accertare e segnalare la corrispondenza o meno fra identificatore univoco di messaggio associato al messaggio ricevuto e risultato della detta decodifica dell'identificativo di controllo.

Sempre secondo l'invenzione, si è anche pensato di realizzare un sistema per una verifica di sicurezza di un messaggio trasmesso e ricevuto in forma elettronica, il quale dal lato trasmittente comprende un generatore di identificativo univoco di messaggio; un dispositivo di codifica che riceve l'identificativo di messaggio prodotto dal generatore e lo codifica secondo un codice associato al titolare del messaggio da trasmettere, per ottenere da esso un identificatore di controllo della

identità del titolare del messaggio; mezzi di trasmissione che associano al messaggio da trasmettere l'identificatore di controllo e l'identificatore univoco di messaggio ottenuti; e dal lato ricevente comprende, per la verifica di sicurezza di un messaggio ricevuto: un dispositivo di controllo che verifica e segnala che l'identificatore di messaggio associato al messaggio ricevuto è stato o non è stato già ricevuto precedentemente; un dispositivo di decodifica che riceve l'identificatore di controllo del titolare associato al messaggio ricevuto e applica ad esso una decodifica associata ad un supposto titolare del messaggio ricevuto; mezzi di verifica che accertano e segnalano la corrispondenza o meno dell'identificatore univoco di messaggio con il risultato della decodifica dell'identificativo di controllo.

Sempre secondo l'invenzione, si è anche pensato di realizzare un dispositivo per l'associazione di elementi di verifica di sicurezza ad un messaggio trasmesso in forma elettronica, caratterizzato dal fatto di comprendere: un generatore di identificativo univoco di messaggio; un dispositivo di codifica che riceve l'identificativo di messaggio prodotto dal generatore e lo codifica secondo un codice associato al titolare del messaggio da trasmettere, per ottenere da esso un identificatore di controllo della identità del titolare del messaggio; mezzi che associano al messaggio da trasmettere l'identificatore di controllo e l'identificatore univoco di messaggio ottenuti.

Per rendere più chiara la spiegazione dei principi innovativi della presente invenzione ed i suoi vantaggi rispetto alla tecnica nota si descriverà di seguito, con l'aiuto dei disegni allegati, una possibile realizzazione esemplificativa applicante tali principi. Nei disegni:

-figura 1 rappresenta uno schema a blocchi di un dispositivo, o parte dal lato trasmittente, di un sistema di verifica di sicurezza realizzato secondo l'invenzione;

-figura 2 rappresenta uno schema a blocchi di un dispositivo, o parte dal lato ricevente, di un sistema di verifica di sicurezza realizzato secondo l'invenzione;

-figura 3 rappresenta schematicamente una possibile combinazione di informazioni secondo il metodo della presente invenzione.

Con riferimento alle figure, in figura 1 è mostrata la parte dal lato trasmittente (indicata genericamente con 10) di un sistema di sicurezza realizzato secondo l'invenzione. Tale parte o dispositivo 10 comprende un generatore 11 per la generazione di un identificativo univoco di messaggio (indicato con ID_{Msg}) e un dispositivo di codifica 12 che riceve l'identificativo di messaggio ID_{Msg} prodotto dal generatore e lo codifica per ottenerne una sua versione codificata, chiamata qui identificatore ID_{CR}, la quale sarà impiegabile, come sarà chiaro nel seguito, come identificatore di controllo della identità del titolare del messaggio.

Il dispositivo 10 è associato ad un noto sistema 13 (qui non descritto, essendo ben noto e facilmente immaginabile dal tecnico) per la produzione di messaggi Msg da trasmettere e ai quali si vuole garantire la sicurezza offerta dalla presente invenzione. Tali messaggi possono essere tradizionali messaggi elettronici per la gestione di transazioni monetarie, ad esempio di un circuito di carte di credito o di debito.

Il generatore 11 è un noto generatore di chiavi uniche. Esso può essere realizzato sia hardware che software (ad esempio, il noto GUID generator di Microsoft). Il suo principio di funzionamento si basa sulla generazione casuale di una chiave ID sufficientemente lungo da rendere virtualmente nulla la probabilità di generare due chiavi identiche. Per ogni messaggio da inviare, il generatore produce perciò un identificatore (che può essere rappresentato con una sequenza di bit, numeri, caratteri, ecc.) che è unico e non sarà mai più impiegato. Ciò assicura che non esistano chiavi "gemelle".

L'ID del messaggio (che può essere chiamato anche LEFT KEY) è da intendersi quindi come una chiave sicuramente ma prodotta prima e quindi una chiave nuova.

Il dispositivo di codifica 12 codifica l'ID_{Msg} in modo da ottenere un identificativo ID_{CR} che contiene in modo mascherato l'ID_{Msg} permettendo, conoscendo la giusta decodifica, di risalire ad esso o comunque ad una sua rappresentazione che permette di conoscere se ID_{CR} è realmente stato creato tramite corretta codifica di ID_{Msg}. L'ID_{CR} può essere anche chiamato RIGHT KEY.

Ad un messaggio Msg vengono così associati i due identificativi (unici per ciascun messaggio) ID_{Msg} e ID_{CR}. Come sarà chiaro nel seguito, il primo permette di riconoscere l'unicità di un messaggio, il secondo permette di avere la conferma dell'identità del titolare che ha prodotto o a cui si riferisce il messaggio.

Infatti, la codifica di ID_{Msg} in ID_{CR} viene eseguita secondo un codice che è stato preventivamente associato al titolare del messaggio da trasmettere. Ad esempio, è vantaggioso che la codifica (e la successiva corrispondente decodifica) vengano realizzate come operazioni di crittazione e decrittazione a chiave, con una particolare chiave o algoritmo associato al particolare titolare del messaggio. In particolare, tali crittazione e decrittazione possono vantaggiosamente essere del noto tipo a chiave pubblica/privata in cui la crittazione viene eseguita dal dispositivo crittografico 12 impiegando la chiave segreta privata del titolare che invia, o a cui si riferisce, il messaggio.

Una volta ottenuti gli identificativi da associare al messaggio essi possono essere inviati alla parte ricevente del sistema attraverso un adatto noto mezzo trasmissivo (ad esempio internet, reti dedicate, linee telefoniche, ecc.). I mezzi di trasmissione e i percorsi seguiti dai vari identificativi e dal messaggio possono essere gli stessi per tutti o essere differenti fra loro a seconda di specifiche esigenze o desideri.

ID_{Msg} e ID_{CR} possono anche essere assemblati in un unico identificatore composto ID_T (che può anche essere chiamato SUPER KEY= LEFT KEY+ RIGHT KEY)

Nel caso di uso di un unico mezzo trasmissivo gli identificativi e il messaggio possono essere assemblati in un unico messaggio totale MSG_T. Tutto ciò è mostrato chiaramente nella figura 3. Se desiderato, tale messaggio totale può essere a sua volta crittografato secondo tecniche note.

In una realizzazione dell'invenzione, al messaggio viene anche associato un identificativo $ID_{titolare}$, unico per ciascun possibile titolare del messaggio da trasmettere. Ad esempio, nel caso di una transazione tramite carta di credito, tale $ID_{titolare}$ può essere il numero di carta. Tale $ID_{titolare}$ può essere prodotto o estratto da mezzi 14, ad esempio una memoria elettronica programmata, mezzi di immissione manuale o mezzi di lettura di dati di titolare presenti su una carta impiegata nella transazione. Tale $ID_{titolare}$ può anche essere impiegato per comandare la giusta codifica nel dispositivo di codifica 12

Possono essere impiegati noti metodi di combinazione delle varie parti e note eventuali codifiche di trasmissione, anche dipendenti dal particolare mezzo di trasmissione e anche desiderate per implementare ulteriori livelli di sicurezza. Tutto ciò è facilmente immaginabile dal tecnico esperto e non sarà qui ulteriormente descritto o mostrato.

In figura 2 è mostrata la parte (indicata genericamente con 16) del sistema secondo l'invenzione presente sul lato ricevente il messaggio.

Per la verifica di sicurezza di un messaggio (Msg) ricevuto (e che può essere processato, secondo l'uso al quale è destinato il messaggio, da un qualsivoglia noto sistema di trattamento 17, ad esempio, un gestore di transazioni, qui non ulteriormente descritto) tale parte ricevente 16 comprende un dispositivo di controllo

18 per riconosce se un ID_{Msg} associato ad un messaggio ricevuto non era già stato precedentemente ricevuto. Per il riconoscimento, il dispositivo 18 gestisce un archivio 19 di ID già usati. Ogniqualvolta arriva un ID_{Msg} il dispositivo controlla nell'archivio 19 se esso è già stato memorizzato ed emette un corrispondente segnale 20 di ID accettabile o di ID non accettabile. Se l'ID non era ancora stato usato il messaggio associato è considerato nuovo e l'ID viene memorizzato nell'archivio per impedirne un nuovo uso futuro.

La parte ricevente 16 comprende anche un dispositivo di decodifica 21 che riceve l'identificatore di controllo del titolare ID_{CR} associato al messaggio ricevuto e applica ad esso una decodifica associata ad un supposto titolare del messaggio ricevuto. In uscita dal decodificatore si ottiene così un identificatore ID_{DCR}. La decodifica è realizzata in modo tale che vi è una prestabilita corrispondenza fra ID_{Msg} e ID_{DCR} se il ID_{CR} era stato ottenuto per codifica del ID_{Msg} con il metodo associato al titolare del messaggio.

Mezzi di verifica 22 ricevono l'ID_{Msg} e ID_{DCR} e accertano e segnalano con un segnale 23 l'esistenza o meno di tale prestabilita corrispondenza. Se esiste la corrispondenza il messaggio può essere ritenuto appartenere al legittimo proprietario. Se sono verificate positivamente entrambe le condizioni alle uscite 20 e 23, il dispositivo 16 emette un segnale 24 di verifica positiva e il messaggio Msg associato agli identificativi ricevuti può essere ritenuto accettabile in base alla verifica di sicurezza secondo l'invenzione.

Come si vede sempre in figura 2, il segnale di corrispondenza 23 può essere anche inviato al riconoscitore di ID unico 18 in modo da inibire la memorizzazione dell'ID di messaggio fra gli ID già usati nel caso non sia riscontrata la corrispondenza fra ID_{Msg} e ID_{CR}. Ciò evita di memorizzare inutilmente fra gli ID già usati degli ID

"falsi".Il dispositivo di decodifica 21 opererà in genere in maniera inversa al dispositivo di codifica 12, nel senso che se il codificatore 12 otterrà un certo ID_{CR} da uno specifico ID_{Msg} il decodificatore riotterrà lo stesso ID_{Msg} a partire da quell'ID_{CR}. In tale caso, la verifica di corrispondenza operata dal dispositivo 22 sarà una verifica di uguaglianza fra ID_{Msg} ricevuto e ID_{CR} decodificato.

Se come sopra detto, il codificatore opera una crittazione a chiave, il decodificatore opererà una corrispondente decrittazione a chiave. Le chiavi associate ai titolari saranno memorizzate in un apposito archivio di chiavi 25.

Ad esempio, se il sistema è di crittazione scelto è a chiave pubblica/privata, il decodificatore opererà una decrittazione come previsto da tale sistema noto, impiegando l'opportuna chiave corrispondente al titolare associato al messaggio.

Secondo un aspetto dell'invenzione, se dal lato trasmittente al messaggio da trasmettere viene associato anche il già menzionato identificatore di titolare ($ID_{titolare}$) dal lato ricevente la decodifica da applicare può essere vantaggiosamente selezionata fra una pluralità di possibili decodifiche sulla base dell'identificatore di titolare stesso associato al messaggio ricevuto. La selezione della giusta chiave nell'archivio 25 diviene così molto più rapida, l'$ID_{titolare}$ venendo fornito al dispositivo di decrittazione 21 come indice di ricerca della giusta chiave nell'archivio di chiavi 25.

A questo punto è chiaro come sia possibile realizzare un dispositivo 10 per l'associazione di elementi di verifica di sicurezza ad un messaggio trasmesso in forma elettronica, un sistema 10, 16 per una verifica di sicurezza di un messaggio trasmesso e ricevuto in forma elettronica, e un metodo per una verifica di sicurezza di un messaggio trasmesso e ricevuto in forma elettronica.

Come facilmente immaginabile dal tecnico, la realizzazione pratica può essere totalmente software, totalmente hardware o mista.

Il dispositivo 10 può anche esse realizzato in forma portatile (ad esempio una smart card) da fornire, ad esempio, ad un titolare di carta di credito che può così generare un ID_T o SUPER KEY da fornire insieme agli altri dati (importo da addebitargli, numero di carta, ecc.) per un pagamento tramite la carta. Tali dati possono essere considerati il messaggio MSG ed eventualmente crittografati secondo sistema noto.

In alternativa, il dispositivo potrà essere presso il negozio dove si effettua l'acquisto e il titolare della carta potrà immette in esso in modo riservato la chiave di codifica per la produzione della parte RIGHT KEY della SUPER KEY che verrà così generata dall'apparecchio.

Dalla descrizione sopra fatta risulta evidente la sicurezza del sistema secondo l'invenzione.

Le SUPER KEY sono da ritenersi pubbliche, venendo trasmesse su canali che sono intrinsecamente insicuri, ma nascondo al loro interno in modo protetto, l'univocità sia del messaggio sia del proprietario.

Un ente fornitore del servizio sopra descritto può fornire al cliente un adeguato supporto hardware e/o software (anche integrato direttamente in una carta di credito "intelligente") e il cliente, tramite tale supporto, è in grado di inviare la SUPER KEY (generata sia tramite postazione privata sia tramite postazione pubblica). La SUPER KEY può percorrere (nell'esempio della transazione monetaria) le stesse tappe che percorre l'informazione della normale carta di credito o di debito. La SUPER KEY, una volta utilizzata, è registrata nel database dell'ente e diviene quindi inattiva. Chiunque provasse a riutilizzarla renderebbe nulla la richiesta e l'intercettazione della SUPER KEY non ha quindi alcuna utilità. La SUPER KEY si può anche intendere come "garanzia monouso" di identità.

Un utente scorretto potrebbe non usare il proprio generatore di chiavi uniche, ma

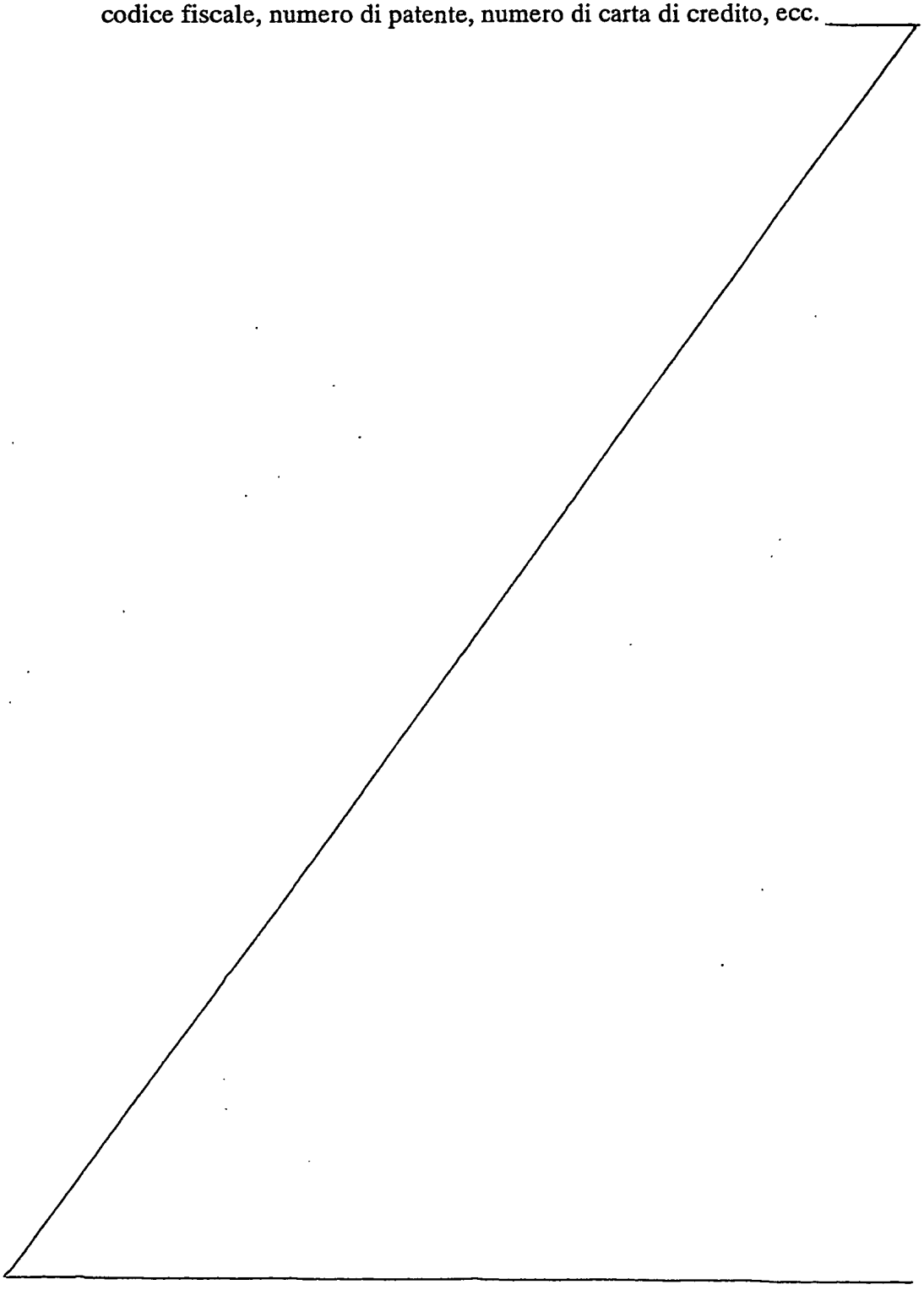
rubare una delle chiavi già prodotte da un'altro utente e crearne così una gemella. La chiave sarebbe però comunque inutilizzabile poiché ogni volta che un utente effettua una transazione sfruttando il generatore di chiavi uniche la chiave generata viene aggiunta alla lista presente nel database dell'ente. Il database contiene l'elenco di tutte le LEFT KEY prodotte nel tempo (e solo le LEFT KEY, non RIGHT KEY e SUPER KEY) e garantisce che le chiavi già prodotte siano inutilizzabili. La prestabilita corrispondenza biunivoca tra l'utente ed il corrispettivo algoritmo o chiave di codifica/decodifica, con il corrispondente archivio di chiavi e/o algoritmi presso l'ente, garantisce poi la possibilità per l'ente di distinguere realmente due utenti e rigettare richieste/messaggi contraffatti. Poiché l'identificatore di unicità del messaggio giunge all'ente sia in chiaro che in forma codificata, risulta impossibile falsificare solo l'identificatore di unicità del messaggio all'interno di una SUPER KEY.

Naturalmente, la descrizione sopra fatta di una realizzazione applicante i principi innovativi della presente invenzione è riportata a titolo esemplificativo di tali principi innovativi e non deve perciò essere presa a limitazione dell'ambito di privativa qui rivendicato.

Ad esempio, il messaggio MSG può essere di qualsiasi tipo noto, anche crittografato per essere decrittato all'arrivo secondo un qualsiasi metodo noto. Tali operazioni possono anche essere eseguite dagli stessi dispositivi 12, 21 che codificano e decodificano l'identificatore di messaggio.

L'identificatore di messaggio può anche essere assemblato al messaggio prima della codifica e la codifica può poi essere eseguita sul risultato dell'assemblaggio per avere un identificatore ID_{CR} inglobato in forma crittografata nel messaggio che viene trasmesso, per essere poi decodificato ed estratto dal lato ricevente.

L'identificatore di titolare può essere un identificatore specifico, assegnato dal gestore del servizio o un identificatore unico già esistente e convenzionalmente scelto. Ad esempio, in caso di titolare persona fisica può essere impiegato il suo codice fiscale, numero di patente, numero di carta di credito, ecc.



RIVENDICAZIONI

1. Metodo per una verifica di sicurezza di un messaggio (Msg) trasmesso e ricevuto in forma elettronica, il quale:
   - dal lato trasmittente comprende le fasi di associare al messaggio, per la sua successiva verifica di sicurezza, un identificatore univoco di messaggio (ID_{Msg}) e un identificatore (ID_{CR}) di controllo della identità del titolare del messaggio, l'identificatore di controllo (ID_{CR}) essendo ottenuto applicando all'identificatore univoco di messaggio (ID_{Msg}) una codifica associata al titolare del messaggio da trasmettere;
   - dal lato ricevente, per la verifica di sicurezza di un messaggio (Msg) ricevuto, comprende le fasi di:
     - verificare e segnalare il fatto di avere o non avere già ricevuto precedentemente un messaggio con lo stesso identificatore univoco di messaggio (ID_{Msg}) associato;
     - applicare una decodifica, associata ad un supposto titolare del messaggio ricevuto, all'identificatore di controllo del titolare (ID_{CR}) associato al messaggio ricevuto;
     - accertare e segnalare la corrispondenza o meno fra identificatore univoco di messaggio (ID_{Msg}) associato al messaggio ricevuto e risultato (ID_{DCR}) della detta decodifica dell'identificativo di controllo (ID_{CR}).
2. Metodo secondo rivendicazione 1, nel quale prima della trasmissione l'identificatore univoco di messaggio (ID_{Msg}) e l'identificatore (ID_{CR}) di controllo della identità del titolare del messaggio sono assemblati in un unico identificatore composto (ID_T).

3. Metodo secondo rivendicazione 1, nel quale dal lato trasmittente, almeno l'identificatore di controllo (ID_{CR}) viene assemblato con il messaggio e trasmesso con esso.
4. Metodo secondo rivendicazione 3, nel quale l'assemblaggio avviene inserendo l'identificatore di messaggio (ID_{Msg}) nel messaggio (Msg) e applicando la codifica al risultato dell'inserimento.
5. Metodo secondo rivendicazione 1, nel quale, dal lato trasmittente, al messaggio da trasmettere viene associato anche un identificatore di titolare ($ID_{titolare}$) e, dal lato ricevente, la decodifica da applicare viene selezionata fra una pluralità di possibili decodifiche sulla base dell'identificatore di titolare ($ID_{titolare}$) associato al messaggio ricevuto.
6. Metodo secondo rivendicazione 1, nel quale la codifica e la decodifica sono operazioni di crittazione e decrittazione a chiave.
7. Metodo secondo rivendicazione 3, nel quale la crittazione e decrittazione è del tipo a chiave pubblica/privata.
8. Metodo secondo rivendicazione 1, nel quale l'accertamento della corrispondenza fra identificatore univoco di messaggio (ID_{Msg}) associato al messaggio ricevuto e risultato della decodifica dell'identificativo di controllo (ID_{CR}) consiste nella verifica dell'uguaglianza fra tale identificatore univoco di messaggio (ID_{Msg}) e il risultato della decodifica dell'identificativo di controllo (ID_{CR}).
9. Sistema per una verifica di sicurezza di un messaggio (Msg) trasmesso e ricevuto in forma elettronica, il quale comprende:
   - dal lato trasmittente:
     - un generatore di identificativo univoco di messaggio (ID_{Msg});

- un dispositivo di codifica che riceve l'identificativo di messaggio (ID_{Msg}) prodotto dal generatore e lo codifica secondo un codice associato al titolare del messaggio da trasmettere, per ottenere da esso un identificatore (ID_{CR}) di controllo della identità del titolare del messaggio;
- mezzi di trasmissione che associano al messaggio da trasmettere l'identificatore di controllo (ID_{CR}) e l'identificatore univoco di messaggio (ID_{Msg}) ottenuti;

- dal lato ricevente, per la verifica di sicurezza di un messaggio (Msg) ricevuto:
  - un dispositivo di controllo che verifica e segnala che l'identificatore di messaggio (ID_{Msg}) associato al messaggio ricevuto è stato o non è stato già ricevuto precedentemente;
  - un dispositivo di decodifica che riceve l'identificatore di controllo del titolare (ID_{CR}) associato al messaggio ricevuto e applica ad esso una decodifica associata ad un supposto titolare del messaggio ricevuto;
  - mezzi di verifica che accertano e segnalano la corrispondenza o meno dell'identificatore univoco di messaggio (ID_{Msg}) con il risultato della decodifica dell'identificativo di controllo (ID_{CR}).

10. Sistema secondo rivendicazione 8, caratterizzato dal fatto che i dispositivi di codifica e di decodifica sono dispositivi di crittazione e di decrittazione a chiave.
11. Sistema secondo rivendicazione 9, caratterizzato dal fatto che i dispositivi di crittazione e di decrittazione sono del tipo a chiave pubblica/privata.

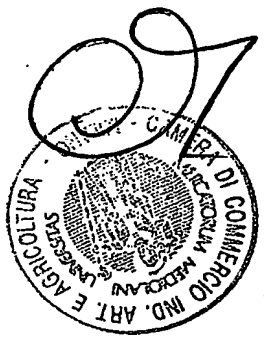
12. Dispositivo per l'associazione di elementi di verifica di sicurezza ad un messaggio trasmesso in forma elettronica, caratterizzato dal fatto di comprendere:

    - un generatore di identificativo univoco di messaggio (ID_{Msg});
    - un dispositivo di codifica che riceve l'identificativo di messaggio (ID_{Msg}) prodotto dal generatore e lo codifica secondo un codice associato al titolare del messaggio da trasmettere, per ottenere da esso un identificatore (ID_{CR}) di controllo della identità del titolare del messaggio;
    - mezzi che associano al messaggio da trasmettere l'identificatore di controllo (ID_{CR}) e l'identificatore univoco di messaggio (ID_{Msg}) ottenuti.

13. Dispositivo secondo rivendicazione 12, caratterizzato dal fatto che il dispositivo di codifica è un dispositivo di crittazione a chiave.

14. Dispositivo secondo rivendicazione 12, caratterizzato dal fatto di emettere un identificatore composto (ID_T) che è formato dalla combinazione dell'identificatore univoco di messaggio (ID_{Msg}) e dell'identificatore (ID_{CR}) di controllo della identità del titolare del messaggio.

I mandatari



Tav.I

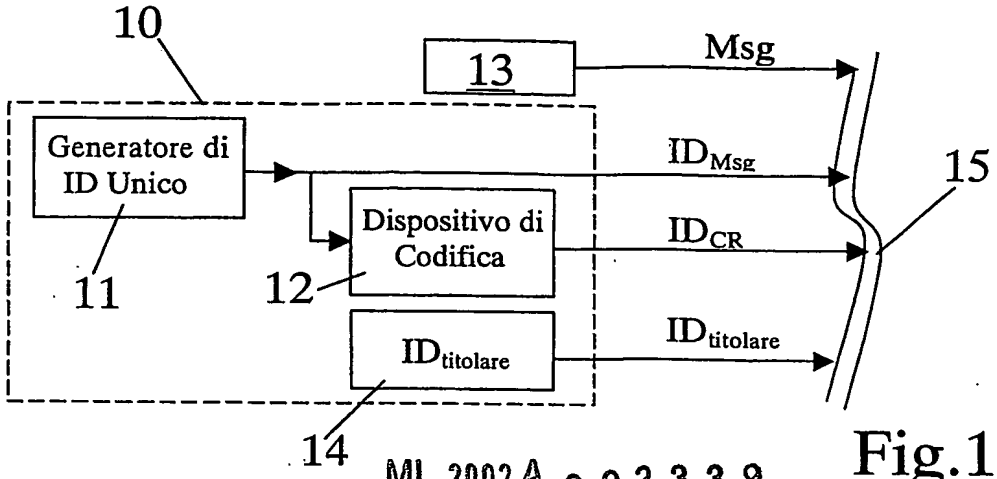


Fig.1

MI 2002 A 002339

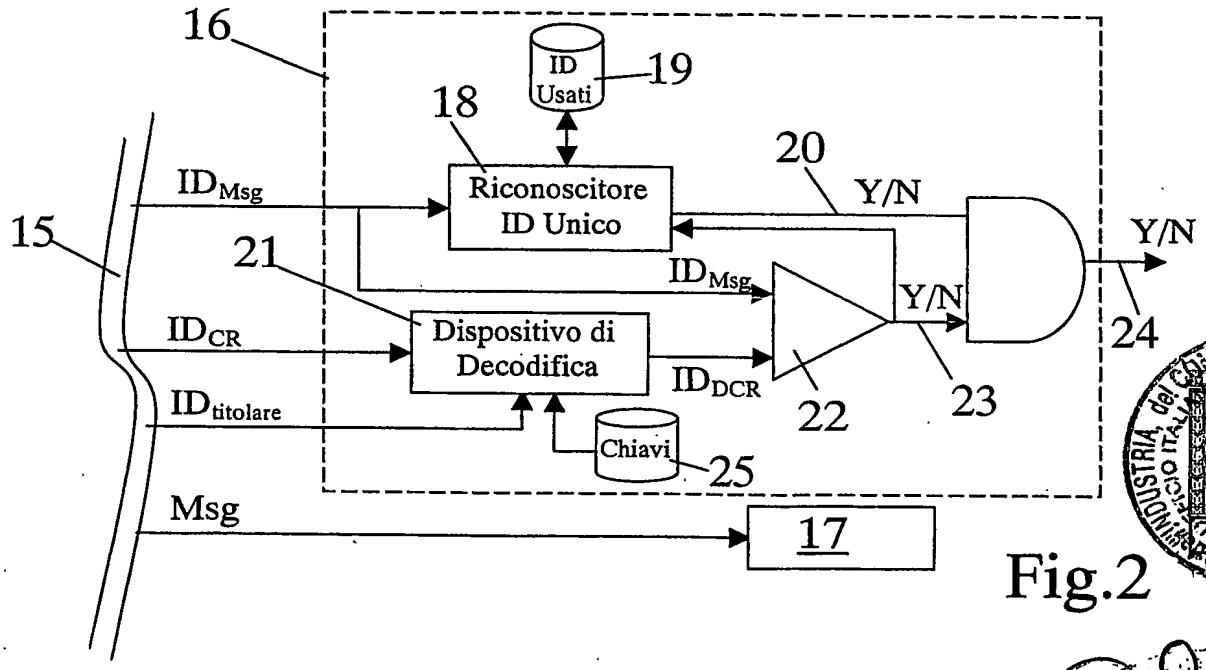


Fig.2

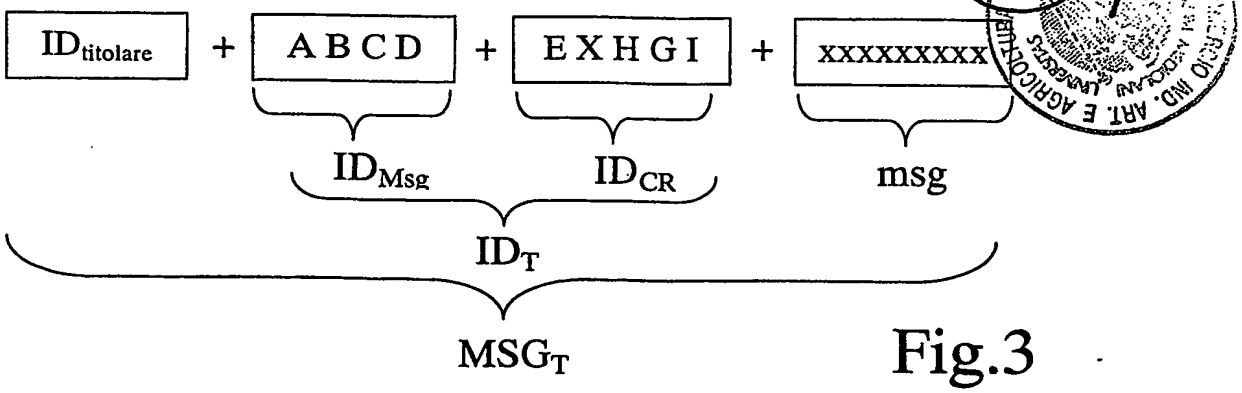


Fig.3

I mandatari